Stanford | Geopolitics, Technology, and Governance
Cyber Policy Center

Win-Win: A Public Private Strategy for Dramatically Improving National Security Tech

A Proposal Developed for the Technology and Public Policy Project[1]

Anthony Vinci
October 17, 2019

Summary

The next presidential term will confront an increasingly urgent question of how to compete with China, economically and militarily. Simply increasing national security funding or R&D spending will not ensure victory against a competitor able to outspend the United States. Instead, we will need once again to revolutionize public-private partnerships to meet the challenge, harnessing more efficient ways of developing and implementing new technology. This paper proposes a novel approach for such partnerships, leveraging a joint venture model to share proprietary federal data with industry—on a limited basis, with appropriate safeguards—to catalyze faster development of new national security technology applications.

Introduction

At a time of increasingly stiff Chinese economic and technological competition, the United States has lost its competitive edge across a range of national security technologies. There are bright spots of technological innovation beyond the commercial state-of-the-art in domains such as space and satellite systems, supercomputing, and weapons technology like hypersonics. Yet, in cloud computing and mobile applications, and other aspects of enterprise IT, the federal government is five to ten years behind industry. U.S. national security technologies lag woefully behind in key areas of competition with China that represent sources of strategic and economic advantage, including artificial intelligence (AI), autonomous vehicles, biotechnology, quantum computing and general IT infrastructure.

[1] Disclaimer: The views and opinions expressed in this paper are solely those of the author and do not necessarily reflect those of Stanford University, the Geopolitics, Technology and Governance Program, or the Technology and Public Policy Project.

The general efficiency and effectiveness of federal, state and local governments are reliant upon information technology, which increasingly lies at the heart of geopolitical competition. Improving basic public sector technology allows all government functions to be more effective, including the defense and intelligence enterprises. Within the national security realm, many of the most important technologies—including computer vision, artificial intelligence, autonomous vehicles and space systems—are 'dual use' technologies. There are also, of course, defense-specific technologies, such as weapon systems, military vehicles, certain aerospace technologies, communications and sensor technologies. Technology innovation must be accelerated throughout this entire spectrum.

China is executing plans to achieve President Xi Jinping's goal of China becoming a "global leader in innovation" by 2035. These include the "Made in China 2025" plan to climb the manufacturing value chain, megaprojects to develop a lead in quantum computing, and the "New Generation Artificial Intelligence Development Plan." Such massive scale development plans are aided by a combination of public and private economic cooperation in the Chinese capitalist-communist system which China calls "civil-military fusion."

In order to compete on the scale necessary to meet China's challenge, the United States must take advantage of the innate entrepreneurial and innovative nature of the American economy and the American government, a unique advantage which authoritarian states cannot replicate. This paper proposes that instead of seeing the government as a consumer, we must also see the government as a partner with industry in joint ventures that strengthen the government and help companies compete, especially in data-driven technology domains that represent key areas of strategic advantage.

The Challenge

The U.S. government has two options to seed innovation for government use: either invent, produce and integrate new technology or enlist the private sector to do it. In most cases, outsourcing innovation makes more sense. While large companies can handle the complexities of government contracting, many of the most innovative technologies come out of smaller companies. Many small companies no longer desire to work with the national security community and government. Technology firms want to own their intellectual property (IP)—an arrangement that government contracting typically precludes—and government contracts often lack the flexibility for the product to be continuously updated, improved, and scaled. In contrast, commercial markets are typically larger and offer the promise of more lucrative returns.

The federal government has two primary means of collaborating with industry: grants and contracts. At the R&D stage Technology Readiness Levels (TRL) 1-3, grants are typically used (Figure 1). Technologies at these stages include basic materials research or fundamental proofs of concept—for example, a new sensor technology. At the development and operations stage (TRL 8-9), technology is fielded—for example, new sensors are affixed to vehicles or new armor is tested on a tank—and contracts are used.

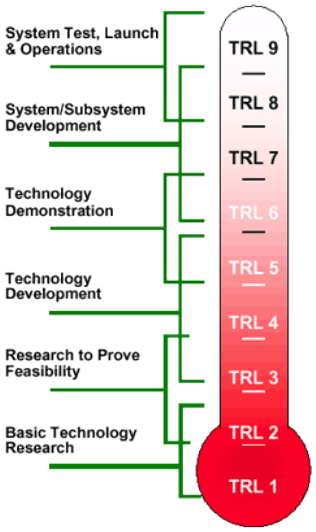

Figure 1: Technology Readiness Level (TRL) scale (Source: NASA)

For certain government requirements, neither contracts nor grants are ideal. For example, TRLs 3-7 require open-ended, creative solutions using technology that works at a basic level and/or exists in other industries.[i]

In particular, it may be important to evolve the product with the government customer, and/or incorporate requirements for flexible scaling to larger and more varied use cases over unpredictable timelines. At these mid-level TRLs, grants are not as useful because they do not lead to production and implementation, while contracts often have the wrong incentive structure because they do not promote or even allow for continued innovation.

How is it possible to incentivize the best technologists to partner with the government to forge valuable solutions? Such an incentive structure would need to solve for a few issues: faster, less rigid contracting, ownership of IP, flexibility and the ability to scale and retain a competitive advantage. Put another way, what might a tenable government public-private partnership approach look like to innovate at the mid-TRL levels and bring technologies into general use?

The Proposal

This proposal offers a new approach capable of overcoming these issues for developing mid-TRL technologies. In the proposed joint venture model, the federal government would contribute technology rights or data, while a company contributes technology talent and expertise capable of determining how to apply the technology. In short, the government 'invests' data sets into a company with the expectation of a 'return' in the form of access to the technology that the company creates by putting that data to work over the duration of a long-term relationship.

Technologies that rely heavily on data are promising targets for government innovation and for public-private joint ventures. While the federal government has a lot of data, it is not very good at figuring out how to use it. Yet many promising technologies—AI and autonomous vehicles, for example—require immense amounts of data to develop. Through the proposed

model, the government obtains better technology delivered faster, while their private sector partners can gain a competitive advantage from unique and large data sets.

Computer Vision Development Example

Consider how an agency like the National Geospatial-Intelligence Agency (NGA) develops and uses artificial intelligence-based computer vision software. NGA is charged with performing intelligence analysis on satellite imagery. The key challenge is that there is too much satellite imagery for human beings to consume via manual tools.

Here, government's traditional approaches have failed: The agency awarded grants to companies and academic institutions to perform computer vision R&D, but little of that technology has been transferred into government use because it is generally too low TRL. Likewise, traditional contractors have been engaged to produce the computer vision technology. But the contracts take 12 to 18 months to be awarded and then months or years to execute. By the time the technology is developed and produced, the government's requirements for the technology have changed and the technology itself has evolved to make the original proposed solutions irrelevant and incompatible.

In the proposed joint venture model, NGA might offer to share unique historical imagery data with partner companies, which could use the data to develop new computer vision systems, offering a competitive advantage over other firms. The government would receive the benefits of the technology as well as an ability to tailor new capabilities as additional data is released. This partnership could be carried out at minimal cost to the government as the company would make its profit from selling the capability to third-party customers.

This approach is applicable across a wide spectrum of technologies and use cases. While most obvious for data analytics and artificial intelligence, other relevant areas include autonomous vehicles, logistics, maintenance, process automation, robotics, sensor systems, space, hardware design, and advanced manufacturing. All of these technologies require large datasets for training and optimization. Even outside of these data intensive areas, most traditional industries include some form of machine learning or data analytics in the design phase, operational processes, or for optimization including clean technology, agriculture and transportation. Given that the federal government has so many large and unique data sets available across such wide swaths of industry, sharing data and forming joint ventures would create a competitive boon for many U.S. industries.

The proposed joint venture model could also be applied to civilian federal agencies. Like the national security enterprise, these agencies spend too much and remain years behind the state-of-the-art technology. Applying a joint venture model to national security agencies provides a test of the concept which can then be applied more broadly.

How it Would Work

In the proposed model, the government 'invests' data sets into a company with the expectation of a 'return' in the form of access to the technology that the company creates by putting that data to work over the duration of a long-term relationship. Shared government data would allow the recipient company to develop a competitive advantage while evolving the technology into higher TRLs for use in the commercial as well as government sectors.

Ensuring the security and privacy of any shared data would be central to any joint venture arrangement. This would be done through an internal review by relevant offices (e.g. Counterintelligence and General Council offices). The data would also need to be organized and cleaned to make it useful. This process would be similar to the process that currently occurs when releasing government data for other purposes such as open sourcing, Freedom of Information Act releases or sharing during government sponsored competitions. The government data would also be granted within the bounds of other current regulations on sharing technology and data, such as International Traffic in Arms (ITAR), and companies granted such data would also have to follow these regulations.

During this development stage, the company would have full flexibility to develop and scale the technology. For example, the government may provide imagery for the purpose of a computer vision algorithm to detect certain types of military equipment. In working with the data, the company could ultimately determine that the data is actually best suited to detect civilian infrastructure. The company would require this flexibility. In turn, as novel applications are developed, the government would have a right to use that technology.

Once the technology achieves a sufficiently high TRL to be useful and scalable, the government would provide a contract to the company to bring the technology to production. Meanwhile, the company would have the freedom to develop products out of this data, so it might come up with something much later or combine it with other datasets into unrelated products. During this entire process, the data would be treated as proprietary and therefore secured jointly between the company and government. Moreover, the company would have certain limits on what it could do with the data as it relates to sharing it or developing products derived from it for certain customers, e.g. the company could not sell the data or a product to a Chinese buyer.[ii]

The Brokerage

To facilitate the joint venture model, a third party 'broker' should be created to find the right partners, bring them together, and help create and manage the relationship. The organization would ideally be set up as a non-profit, although a federally funded research and development center (FFRDC), or a government-owned company could also perform this function. The

brokerage would be governed by a joint board composed of commercial and government officers. The organization would have the following six functions:

1. Work with government partners to identify the data or other shareable technology that might form the basis of a joint venture.
2. Find companies, academic institutions, non-profits or individual inventors that are interested in access to the data.
3. Match the two (or more) parties with mutual interest. If there are more than two companies with an interest, determine whether to have multiple partners or to undertake a competitive process. The competitive process would look less like those under the federal acquisition regulations (FAR) than, for example, a competition in which the brokerage might give data to multiple companies and choose the best product after a 'bake off.'
4. Act as the objective 'middle person' to help the parties negotiate common goals and the specifics of a joint venture relationship.
5. Draw up the contract between the two parties, including adding standard best practices into the agreement, such as how to secure the data.
6. Monitor the relationship in order to verify that both parties carry it out as stipulated and arbitrate if there is a disagreement.

Phased Implementation

This joint venture model can be carried out in three phases:

In the first phase, it should be tested at one or a few agencies. NGA would be a good place to start due to its significant usable data and history of working well in public-private partnership contexts. Other potential first customers might be the Air Force through its new CTO office or Army Futures Command. The agency(ies) could use current Broad Agency Announcement (BAA) and Other Transaction Authority (OTA) authorities to carry out this approach, similar to how Intelligence Advanced Research Projects Activity (IARPA) and Defense Innovation Unit (DIU) use such authorities. These authorities should be used until these technologies reach full production, at which point, contracts should be awarded.

In the second phase, a government-funded 'brokerage' would be set up to scale this approach, reliant on Congressional funding support.

In a third phase, contingent on promising results, the approach would be expanded outside of the national security community to civilian government agencies.

Proposed Actions

This policy requires backing by the administration to succeed. It can likely use existing authorities to begin, however, an Executive Order and support from relevant leaders is necessary.

An Executive Order provides the mandate, guidance and backing that agency directors will require to overcome so called 'antibodies.' In particular, the Office of Management and Budget (OMB) and other budgeting offices in the Department of Defense (DoD) and Office of the Director of National Intelligence (ODNI), as well as the General Counsel offices of both the DoD and ODNI are key gatekeepers that generally require support from an administration to allow agencies to pursue a novel approach.

The administration should begin by proposing that a single agency or small group of agencies execute the policy as a means to allow for experimentation and to mitigate risk. NGA, CIA's Directorate of Digital Innovation (DDI), the Air Force's new CTO office and Army Futures Command are all promising candidate organizations that have the culture, data, and expertise necessary to execute.

Therefore, the administration should draft an Executive Order directed at the intelligence community and DoD requiring:

A. The creation of a board of advisors, made up of government and commercial experts, to scope, support and set up this approach.
B. A few agencies to try out the above detailed approach using existing authorities and to improve on the model and report back findings.
C. The creation of a brokerage-like capability which could be used to match company needs for data with government datasets and agencies. Either set up as a non-profit, FFRDC, for profit company, or government owned company (as recommended by the advisory board).
D. The creation of a separate channel, outside of this program, in order to ensure that security and privacy rules are adhered to. This could be a third-party governing body or existent capabilities such as the privacy and counterintelligence offices within the DoD or another department.
E. A flexible legal approach to consummating the partnership between the agency and company, including data and technology rights as well as accountability standards.
F. A set of standards and best practices for agencies to implement in choosing between grant, contract and 'joint venture' approaches to working with businesses.
G. Agencies to use this joint venture model by mandating a certain percentage of technology development through this approach.
H. A set of accountability metrics for the use of this approach.

I. The establishment of executive agents in the DoD and under the DNI for management of this function.

Ultimately, this policy may require legislation to scale. While current authorities or an Executive Order may make the process possible, legislation could make it much more efficient and would make it much more predictable by ensuring authorization and dedicated, continuous funding. As these trial agencies report successes and discover where new legislation is necessary, the administration should work with Congress to fund this approach through the National Defense Authorization Act (NDAA) and Intelligence Authorization Act. In parallel to government action, the administration should work directly with commercial interests to understand their needs better and enlist their support, through the creation of a public-private board of advisors on this topic.

Precedents

Agencies have used a number of related approaches before. For example, NGA attempted to set up a program called GeoWorks to forge private sector partnerships, but it did not work due to an inability to share new data, amongst other factors. Several other approaches to correcting inefficiencies in contracting have been tried, most notably the use of OTAs by DIU and other parts of the DoD, along with In-Q-Tel investments in emerging technology. Likewise, the National Oceanic and Atmospheric Agency (NOAA) 'Big Data Project' used Google and Microsoft to host data on their respective clouds.

The joint venture approach differs in key ways from those attempts. Unlike OTAs, the joint venture model entails actually transferring data or other technology to the company and allowing it to continue to use that data for its own purposes (while continuing to secure it and maintaining certain controls). This approach confers unique benefits and incentives on both government and private sector partners and provides a new tool for leveraging the subset of data that—at a time when government agencies are increasingly focused on making government data public, easily accessible and, machine-readable—would generally not be appropriate for public dissemination.

Risks and Other Considerations

While nearly everyone agrees about the federal government's IT challenges, particularly in the national security community, there is little agreement as to the solution. When it comes to data sharing and joint ventures, the 'sides' of the debate tend to fall on the two ways of sharing government data. On one end of the spectrum are the traditional contractors who are, by and large, accepting of federal acquisition regulations and seek increased contractor spending as the solution for IT challenges. At the other end of the spectrum are those seeking to open source additional data. Government joint ventures challenge both sides to some degree. Those seeking additional contracts fear a net loss in government spending and an inability to

compete with technology companies that might take part in such joint ventures. Those in the open source data community may resist any 'corporate favoritism' or threats to broader government data sharing.

Concerns over corporate favoritism and recommendations to pursue open source approaches should be taken seriously. Open sourcing in the national security context has necessary limits in competition with China and other adversaries. The joint venture model should be implemented alongside open sourcing of additional (non-sensitive or dual-use) datasets. There is a possibility that the initial balance between what should be open sourced, versus contracted, versus going into a joint venture, is not perfect. The government advisory board and brokerage relationship must remain flexible and well connected with grant and contracting authorities in order to find the right balance. A yearly review of the program would also serve to ensure accountability.

Ensuring that the most qualified companies are selected will be critical. Proprietary and classified data must be handled carefully—the data provided to companies will need to remain secure to safeguard privacy protections. Shared data should be cleared through the most stringent measures to ensure that it contains no personally identifiable information (PII) and that minimum-security standards are met in order to protect the data. If it is classified data, the company must have all the proper capabilities to deal with classified access, such as a facility clearance and cleared personnel.

Finally, while any new contracting approach engenders implementation hurdles in the near term, some of this risk can be mitigated through guidelines, training, and other shared knowledge.

Goals and Metrics

Ultimate success will be seen in how fast the national security community can 'catch up' on technology. Metrics of success should include a material increase in the measures of effectiveness of technology operations by agencies, such as faster or better AI systems, and an increase in the speed and agility of agencies to acquire and actually implement new technologies. Currently, it may take 12 to 18 months to contract new technology and even longer for it to be implemented. We should see this shrink closer to commercial standards, which is 6 to 12 months to acquire and implement new technology. A brokerage model delivers greater efficiency because it does not require developing, negotiating, and renegotiating new requirements as the technology evolves.

The receptiveness of the American technology industry will be a major sign of whether this policy is successful. At companies like Google, government contracts spur a wide debate over ethical considerations in the national security domain, which recently occurred over Project Maven. For smaller, start-up companies, substantial concerns exist about burdensome

contracts with the federal government slowing down scaling and depressing valuations. Increasing the number of companies that work with the federal government will be a major metric of success.

Another metric of success will be the use of this new public private-partnership approach to solve national security problems. OTAs were initially used by a small subset of national security offices. Now, OTAs are used by most agencies in one form or another. Similarly, agencies should discover the value of joint ventures and begin to apply them to solving their own unique problems.

Conclusion

During the Cold War with the Soviet Union, the federal government created several new means of partnering with industry and civil society. An entire constellation of actors harnessed U.S. economic might to invent and produce the ideas, technology and weapons necessary to win arms races and outcompete the Soviet Union. Think tanks and FFRDCs like the MITRE Corporation and RAND developed new ideas for technologies and weapon systems designed to meet real or perceived threats. R&D grants via organizations like the Defense Advanced Research Projects Agency (DARPA) provided a means to seed risky new inventions from rockets to the Internet. The Cold War helped launch entire new industries and sources of economic advantage: Silicon Valley, for example, was founded and grew largely in response to the needs of the DoD.

America must once again reconsider how public and private sectors can work together to defend the nation. While there still remains a need for grants and contracts, a third model in the form of joint ventures provides a much-needed avenue for developing and implementing technology for national security and public purposes.

About the Author

Anthony Vinci, PhD, is an Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security (CNAS), a member of MITRE's Board of Trustees Technology Committee and is on the Core Management Team at Bridgewater Associates. He previously served as the Chief Technology Officer (CTO) and Associate Director for Capabilities at the National Geospatial-Intelligence Agency (NGA). Anthony was also on the Senior Steering Group and Executive Committee of Project Maven. He received his Ph.D. in International Relations from The London School of Economics and studied Philosophy at Reed College and the University of Oxford.

Endnotes

[i] For example, a few year ago, technology companies were beginning to apply AI computer vision algorithms to new problems, but they had not yet appeared on the iPhone.
[ii] In practice, such restrictions are already dictated by ITAR, CFIUS and other regulations.